NSTISSI No. 4011
20 June 1994

NSTISS

NATIONAL
SECURITY
TELECOMMUNICATIONS
AND
INFORMATION
SYSTEMS
SECURITY

NATIONAL TRAINING STANDARD FOR INFORMATION SYSTEMS SECURITY (INFOSEC) PROFESSIONALS

NSTISS

NATIONAL SECURITY
TELECOMMUNICATIONS
AND INFORMATION
SYSTEMS SECURITY

NATIONAL MANAGER

FOREWORD

1. This instruction provides the minimum course content for the training of information systems security (INFOSEC) professionals in the disciplines of telecommunications security and automated information systems (AIS) security.

2. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this instruction from:

Executive Secretariat
National Security Telecommunications and
Information Systems Security Committee
National Security Agency
Fort George G. Meade, MD 20755-6000

3. U.S. Government contractors are to contact their appropriate government agency or Contracting Officer Representative regarding distribution of this document.

J. M. McCONNELL
Vice Admiral, U.S. Navy

NSTISSI No. 4011

NATIONAL TRAINING STANDARD FOR INFORMATION SYSTEMS SECURITY (INFOSEC) PROFESSIONALS

SECTION I - PURPOSE

1. This instruction establishes the minimum training standard for the training of information systems security (INFOSEC) professionals in the disciplines of telecommunications and automated information systems (AIS) security.

SECTION II - SCOPE AND APPLICABILITY

2. National Security Telecommunications and Information Systems Security Directive No. 501 establishes the requirement for federal departments and agencies to implement training programs for INFOSEC professionals. As defined in NSTISSD 501, an INFOSEC professional is an individual who is responsible for the security oversight or management of national security systems during phases of the life cycle. That directive is being implemented in a synergistic environment among departments and agencies which are committed to satisfying these INFOSEC education and training requirements in the most effective and efficient manner possible. This instruction is the first in a series of minimum training and education standards which are being developed to assist departments and agencies in meeting their responsibilities in these areas.

3. The body of knowledge listed in this instruction may be obtained from a variety of sources, i.e., the National Cryptologic School, contractors, adaptations of existing department/agency training programs, or a combination of experience and formal training.

4. This instruction is applicable to all departments and agencies of the U.S. Government, their employees, and contractors who are responsible for the security oversight or management of national security systems during each phase of the life cycle.

SECTION III - REFERENCES

5. P.L. 100-235, Computer Security Act of 1987, dated January 8, 1988.

6. National Policy for the Security of National Security Telecommunications and Information Systems, dated July 5, 1990.

7. NSTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, dated 16 November 1992.

8. OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, December 12, 1985.

9. Office of Personnel Management, 5 CFR Part 930, Training Requirements for the Computer Security Act, January 3, 1992.

10. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, June 5, 1992.

SECTION IV - RESPONSIBILITIES

11. Heads of U.S. Government departments and agencies will:

a. Ensure that INFOSEC professionals obtain the body of knowledge as outlined in this instruction.

b. Ensure that an INFOSEC training program is an integral part of the overall training program.

c. Require contractors to comply with the provisions of this instruction when they are responsible for the security oversight or management of national security systems operated by or on behalf of the U.S. Government.

12. The National Manager will:

a. Provide and maintain an INFOSEC training standard to U.S. Government departments and agencies.

b. Ensure that appropriate INFOSEC training courses are developed.

c. Assist other U.S. Government departments and agencies in developing and/or conducting INFOSEC training activities as requested.

SECTION V - TRAINING STANDARD

13. Using a comprehensive model of information systems security, the curriculum is intended to provide two levels of knowledge:

a. Awareness Level. Creates a sensitivity to the threats and vulnerabilities of national security information systems, and a recognition of the need to protect data, information and the means of processing them; and builds a working knowledge of principles and practices in INFOSEC.

b. Performance Level. Provides the employee with the skill or ability to design, execute, or evaluate agency INFOSEC security procedures and practices. This level of understanding will ensure that employees are able to apply security concepts while performing their tasks.

14. The program of instruction, as outlined below, shall encompass scope, suggested sequence, and content.

a. COMMUNICATIONS BASICS (Awareness Level)

Instructional Content	Behavioral Outcomes
- Introduce the evolution of modern communications systems.	- Outline chronology of communications systems and development.

- Describe vehicles of transmission.	- Match features of transmission to descriptors (e.g., signal type, speed production characteristics, etc.)

(1) Topical Content

(a) Historical vs Current Methodology

(b) Capabilities and limitations of various communications systems
- microwave
- line of sight
- satellite
- radio frequency (e.g., bandwidth)
- asynchronous vs synchronous
- dedicated line
- digital vs analog
- public switched network

(1) Topical Content

(a) Historical vs Current Methodology

b. AUTOMATED INFORMATION SYSTEMS (AIS) BASICS (Awareness Level)

Instructional Content	Behavioral Outcomes
- Provide language of an AIS.	- Define terms in an AIS.
- Describe an AIS environment by an AIS.	- Define functions performed.
- Providing an overview of hardware, software, firmware components of an AIS, to integrate into information systems security aspects/ behaviors discussed later.	- Describe interrelationship among AIS components.

(1) Topical Content

(a) Historical vs Current Technology

(b) Hardware
- distributed vs stand-alone
- micro, mini, mainframe processors
- storage devices
- components (e.g., input, output, central processing unit (CPU))

(c) Software
- operating system
- applications

(d) Memory
- sequential
- random
- volatile vs nonvolatile

(e) Media
- magnetic remanence
- optical remanence

(f) Networks
- topology
- sharing of data
- sharing of devices
- file servers
- modems
- asynchronous vs synchronous
- switching

c. SECURITY BASICS (Awareness Level)

Instructional Content	Behavioral Outcomes
- Using the Comprehensive Model of Information Systems Security (contained in the Annex to this instruction), introduce a comprehensive model of information systems security that addresses: - critical characteristics of information	- The student will list and describe the elements of AIS security. - The student will summarize security disciplines used in protecting government automated information systems.

- information states, and - security measures.	- Student will give examples of determinants of critical information.

(1) Topical Content

(a) INFOSEC Overview
- threats
- vulnerabilities
- critical information characteristics
  - confidentiality
  - integrity
  - availability
- information states
  - transmission
  - storage
  - processing
- security countermeasures
  - technology
  - policy, procedures and practices
  - education, training and awareness

(b) Operations Security (OPSEC)
- OPSEC process
- INFOSEC and OPSEC interdependency
- unclassified indicators
- OPSEC surveys/OPSEC planning

(c) Information Security
- policy
- roles and responsibilities
- application dependent guidance

(d) INFOSEC
- cryptography
  - strength (e.g., complexity, secrecy, characteristics of the key)
  - encryption (e.g., point-to-point, network, link)
  - key management (to include electronic key)
- transmission security
- emanations security

- physical, personnel and administrative security
- computer security
  - identification and authentication
  - access control
  - audit
  - object reuse

d. NSTISS BASICS (Awareness Level)

Instructional Content	Behavioral Outcomes
- Describe components (with examples to include: national policy, threats and vulnerabilities, countermeasures, risk management, systems lifecycle management, trust, modes of operation, roles of organizational units, facets of NSTISS.	- Outline national NSTISS Policies. - Cite examples of threats and vulnerabilities of an AIS. - Give examples of Agency implementation of NSTISS policy, practices and procedures.

(1) Topical Content

(a) National Policy and Guidance
- AIS security
- communications security
- protection of information
- employee accountability for agency information

(b) Threats to and Vulnerabilities of Systems
- definition of terms (e.g., threats, vulnerabilities, risk)
- major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring)
- threat impact areas

(c) Legal Elements
- fraud, waste and abuse
- criminal prosecution
- evidence collection and preservation
- investigative authorities

(d) Countermeasures
- cover and deception
- HUMINT
- monitoring (e.g., data, line)
- technical surveillance countermeasures
- education, training, and awareness
- assessments (e.g., surveys, inspections)

(e) Concepts of Risk Management
- threat and vulnerability assessment
- cost/benefit analysis of controls
- implementation of cost-effective controls
- consequences (e.g., corrective action, risk assessment)
- monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information)

(f) Concepts of System Life Cycle Management
- requirements definition (e.g., architecture)
- development
- demonstration and validation (testing)
- implementation
- security (e.g., certification and accreditation)
- operations and maintenance (e.g., configuration management)

(g) Concepts of Trust
- policy
- mechanism
- assurance

(h) Modes of Operation
- dedicated
- system-high
- compartmented/partitioned
- multilevel

(i) Roles of Various Organizational Personnel
- senior management
- program or functional managers
- system manager and system staff
- telecommunications office and staff
- security office
- COMSEC custodian
- INFOSEC Officer
- information resources management staff
- audit office
- OPSEC managers
- end users

(j) Facets of NSTISS
- protection of areas
- protection of equipment
- protection of passwords
- protection of files and data
- protection against malicious logic
- backup of data and files
- protection of magnetic storage media
- protection of voice communications
- protection of data communications
- protection of keying material
- application of cryptographic systems
- transmission security countermeasures (e.g., callsigns, frequency, and pattern forewarning protection)
- reporting security violations

e. SYSTEM OPERATING ENVIRONMENT (Awareness Level)

Instructional Content	Behavioral Outcomes
- Outline Agency specific AIS and telecommunications systems.	- Summarize Agency AIS and telecommunications systems in operation.
- Describe Agency “control points“ for purchase and maintenance of Agency AIS and telecommunications systems.	- Give examples of current Agency AIS/telecommunications systems and configurations.

- Review Agency AIS and telecommunications security policies.

- List Agency-level contact points for AIS and telecommunications systems and maintenance.
- Cite appropriate policy and guidance.

(1) Topical Content

(a) AIS
- hardware
- software
- firmware

(b) Telecommunications Systems
- hardware
- software

(c) Agency Specific Security Policies
- guidance
- roles and responsibilities
- points of contact

(d) Agency Specific AIS and Telecommunications Policies
- points of contact
- references

f. NSTISS PLANNING AND MANAGEMENT (Performance Level)

Instructional Content	Behavioral Outcomes
- Discuss practical performance measures employed in designing security measures and programs. - Introduce generic security planning guidelines/documents.	- Builds a security plan that encompasses NSTISS components in designing protection/security for an instructor-supplied description of an AIS telecommunications system.

(1) Topical Content

(a) Security Planning
- directives and procedures for NSTISS policy
- NSTISS program budget
- NSTISS program evaluation
- NSTISS training (content and audience definition)

(b) Risk Management
- information identification
- roles and responsibilities of all the players in the risk analysis process
- risk analysis and/or vulnerability assessment components
- risk analysis results evaluation
- corrective actions
- acceptance of risk (accreditation)

(c) Systems Life Cycle Management
- management control process (ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications)
- evaluation of sensitivity of the application based upon risk analysis
- determination of security specifications
- design review and systems test performance (ensure required safeguards are operationally adequate)
- systems certification and accreditation process
- acquisition

(d) Contingency Planning/Disaster Recovery
- contingency plan components
- agency response procedures and continuity of operations

- team member responsibilities in responding to an emergency situation
- guidelines for determining critical and essential workload
- determination of backup requirements
- development of procedures for off-site processing
- development of plans for recovery actions after a disruptive event
- emergency destruction procedures

g. NSTISS POLICIES AND PROCEDURES (Performance Level)

Instructional Content	Behavioral Outcomes
- List and describe: specific technological, policy, and educational solutions for NSTISS.	- Playing the role of either a system penetrator or system protector, the student will discover points of exploitation and apply appropriate countermeasures in an instructor-supplied description of an Agency AIS/telecommunications system.
- List and describe: elements of vulnerability and threat that exist in an AIS/ telecommunications system with corresponding protection measures.	

(1) Topical Content

(a) Physical Security Measures
- building construction
- alarms
- information systems centers
- communications centers
- shielding
- cabling
- filtered power
- physical access control systems (key cards, locks and alarms)
- stand-alone systems and peripherals
- environmental controls (humidity and air conditioning)
- fire safety controls
- storage area controls
- power controls (regulator, uninterrupted power service (UPS), and emergency poweroff switch)
- protected distributed systems

(b) Personnel Security Practices and Procedures
- position sensitivity
- employee clearances
- access authorization/verification (need-to-know)
- security training and awareness (initial and refresher)
- systems maintenance personnel
- contractors

(c) Software Security
- configuration management
  - programming standards and controls
  - documentation
  - change controls
- software security mechanisms to protect information
  - segregation of duties
  - concept of least privilege
  - identification and authentication
  - access privileges
  - internal labeling
  - application security features
  - audit trails and logging
  - operating systems security features
  - need-to-know controls
  - malicious logic protection
- assurance

(d) Network Security
- public vs private
- dial-up vs dedicated
- privileges (class, nodes)
- traffic analysis
- end-to-end access control

(e) Administrative Security Procedural Controls
- external marking of media
- destruction of media
- sanitization of media
- construction, changing, issuing and deleting passwords
- transportation of media
- reporting of computer misuse or abuse
- preparation of security plans
- emergency destruction
- media downgrade and declassification
- copyright protection and licensing
- documentation, logs and journals
- attribution
- repudiation

(f) Auditing and Monitoring
- effectiveness of security programs
- conducting security reviews
- verification, validation, testing, and evaluation processes
- monitoring systems for accuracy and abnormalities
- investigation of security breaches
- review of audit trails and logs
- review of software design standards
- review of accountability controls
- privacy

(g) Cryptosecurity
- encryption/decryption method, procedure, algorithm
- cryptovariable or key
- electronic key management system

(h) Key Management
- identify and inventory COMSEC material
- access, control and storage of COMSEC material
- report COMSEC incidents
- destruction procedures for COMSEC material
- key management protocols (bundling, electronic key, over-the-air rekeying)

(i) Transmission Security
- frequency hopping
- masking
- directional signals
- burst transmission
- optical systems
- spread spectrum transmission
- covert channel control (crosstalk)
- dial back
- line authentication
- line-of-sight
- low power
- screening
- jamming
- protected wireline

(j) TEMPEST Security
- shielding
- grounding
- attenuation
- banding
- filtered power
- cabling
- zone of control/zoning
- TEMPEST separation

Enclosure:
Information Systems Security: A Comprehensive Model

ANNEX

INFORMATION SYSTEMS SECURITY: A COMPREHENSIVE MODEL [1]

INTRODUCTION

This Annex serves as a comprehensive model for the security of information systems and also functions as an assessment, systems development, and evaluation tool. The model is unique in that it stands independent of technology. Its application is universal and is not constrained by organizational differences. As with all well-defined fundamental concepts, it is unnecessary to alter the premise even as technology and human understanding evolve.

Computers communicate. Communications systems compute. The evolution of technology has long since eliminated any arbitrary distinction between a computer and its communication components or a communications network and its computing system. Some organizations have attempted to deal with the phenomenon by marrying these functions under common leadership. This has resulted in hyphenated job descriptions such as Computer-Communications Systems Staff Officer and names like Information Technology Group. Unfortunately, these names can mask an inappropriate or poorly executed realignment of organizational responsibilities. Ideally, management will recognize there is a theoretical as well as organizational impact.

The same is true for the security disciplines. Merely combining the communications security (COMSEC) and computer security (COMPUSEC) disciplines under an umbrella of common management is unacceptable. Even if we address the other, albeit less technical, aspects of information systems security such as policy, administration, and personnel security, we still fail to develop a comprehensive view of this evolving technology. The reason for this becomes clear when we are reminded it's the information that is the cornerstone of information systems security. In this sense, any paradigm which emphasizes the technology at the expense of information will be lacking.

---

1. Capt John R. McCumber, Joint Staff, as extracted from the proceedings of the 14th National Computer Security Conference, October 1991.

THE NATURE OF INFORMATION

Defining the nature of information could be a tedious task. To some it represents the free flowing evolution of knowledge; to others, it is intelligence to be guarded. Add to this the innumerable media through which the information is perceived and we have a confusing array of contradictions. How can we present a study of information that has universal application?

It may be best to develop a simple analogy. The chemical compound H^2O means many things to all of us. In its liquid state, water means life-giving sustenance to a desert-dwelling Bedouin; to a drowning victim, it is the vehicle of death. The same steam we use to prepare vegetables could scald an unwary cook. Ice can impede river-borne commerce on the Mississippi River or make a drink more palatable. Science, therefore, does not deal with the perception of the compound, but with its state.

As the compound H^2O can be water, ice or steam, information has three basic states. At any given moment, information is being transmitted, stored, or processed. The three states exist irrespective of the media in which information resides. This subtle distinction ultimately allows us to encompass all information systems technology in our model.

It is possible to look at the three states in microcosm and say that processing is simply specialized state combinations of storage and transfer; so, in fact, there are only two possible states. By delving to this level of abstraction, however, we go beyond the scope and purpose of the model. The distinction between the three states is fundamental and necessary to accurately apply the model. For example, cryptography can be used to protect information while it's transferred through a computer network and even while it is stored in magnetic media. However, the information must be available in plaintext (at least to the processor) in order for the computer to perform the processing function. The processing function is a fundamental state that requires specific security controls.

When this information is needed to make a decision, the end user may not be aware of the number of state changes effected. The primary concern will be certain characteristics of the information. These characteristics are intrinsic and define the security-relevant qualities of the information. As such, they are the next major building block of our information systems security model.

CRITICAL INFORMATION CHARACTERISTICS

Information systems security concerns itself with the maintenance of three critical characteristics of information: confidentiality (Pfleeger's "secrecy"), integrity, and availability [PFL89]. These attributes of information represent the full spectrum of security concerns in an automated environment. They are applicable for any organization irrespective of its philosophical outlook on sharing information.

CONFIDENTIALITY

Confidentiality is the heart of any security policy for an information system. A security policy is the set of rules that, given identified subjects and objects, determines whether a given subject can gain access to a specific object [DOD85]. In the case of discretionary access controls, selected users (or groups) are controlled as to which data they may access. Confidentiality is then the assurance that access controls are enforced. Confidentiality is used instead of secrecy to avoid unwarranted implications that this is solely the domain of governments.

All organizations have a requirement to protect certain information. Even owners of a clearinghouse operation or electronic bulletin need the ability to prevent unwanted access to supervisory functions within their system. It's also important to note the definition of data, which must be protected with confidentiality controls, is broadening throughout government [OTA87]. Actual information labeling and need-to-know imperatives are aspects of the system security policy that are enforced to meet confidentiality objectives. The issue of military versus civilian security controls is one which need not impact the development of a comprehensive representation of information systems security principles.

INTEGRITY

Integrity is perhaps the most complex and misunderstood characteristic of information. We seem to have a better foundation in the development of confidentiality controls than those which can help ensure data integrity. Pfleeger defines integrity as "assets" (which) can only be modified by authorized parties" [PFL89]. Such a definition unnecessarily confines the concept to one of access control.

A much broader definition is used here. Data integrity is a matter of degree (as is the concept of “trust“ as applied to trusted systems) that has to be defined as a quality of the information and not as who does/does not have access to it. Integrity is that quality of information that identifies how closely the data represent reality. How closely does your resume reflect “you?“ Does the credit report accurately reflect the individual’s historical record of financial transactions? The definition of integrity must include the broad scope of accuracy, relevancy, and completeness.

Data integrity calls for a comprehensive set of aids to promote accuracy and completeness as well as security. This is not to say that too much information can’t be a problem. Data redundancy and unnecessary records present a variety of challenges to system implementors and administrators. The users must define their needs in terms of the information necessary to perform certain functions. Information systems security functions help ensure this information is robust and (to the degree necessary) reflects the reality it is meant to represent.

AVAILABILITY

Availability is a coequal characteristic with confidentiality and integrity. This vital aspect of security ensures the information is provided to authorized users when it’s requested or needed. Often it’s viewed as a less technical requirement that is satisfied by redundancies within the information system such as back-up power, spare data channels, and parallel data bases. This perception, however, ignores one of the most valuable aspects of our model that this characteristic provides. Availability is the check-and-balance constraint on our model. Because security and utility often conflict, the science of information systems security is also a study of subtle compromises.

As well as ensuring system reliability, availability acts as a metric for determining the extent of information systems security breaches [DOJ88]. Ultimately, when information systems security preventive measures fail, remedial action may be necessary. This remedial activity normally involves support from law enforcement or legal departments. In order to pursue formal action against people who abuse information systems resources, the ability to prove an adverse impact often hinges

on the issue of denying someone the availability of information resources. Although violations of information confidentiality and integrity can be potentially more disastrous, denial of service criteria tend to be easier to quantify and thus create a tangible foundation for taking action against violators [CHR90].

The triad of critical information characteristics covers all aspects of security-relevant activity within the information system. By building a matrix with the information states (transmission, storage, processing) positioned along the horizontal axis and the critical information (confidentiality, integrity, availability) characteristics aligned down the vertical, we have the foundation for the model.

SECURITY MEASURES

We've now outlined a matrix that provides us with the theoretical basis for our model. What it lacks at this stage is a view of the measures we employ to ensure the critical information characteristics are maintained while information resides in or moves between states. It's possible, at this point, to perceive the chart as a checklist. At a very high level of abstraction, one could assess the security posture of a system by using this approach. For example, you may single out systems information confidentiality during transmission or any intersection area for scrutiny.

The two-dimensional matrix also has another less obvious utility. We can map various security technologies into the nine boxes. Using our example from above, we note it is necessary to protect the confidentiality of the information during its transmission state. We can then determine which security technologies help ensure confidentiality during transmission of the information. In this case, cryptography would be considered a primary security technology. We can then place various cryptographic techniques and products within a subset in this category. Then we repeat the process with other major types of technology that can be placed within these spaces. The procedure is repeated for all nine blocks on our grid. Thus we form the first of three layers which will become the third dimension of our model--security measures.

TECHNOLOGY

The technology layer will be the primary focus of the third dimension. We will see that it provides the basis for the other two layers. For our purposes, we can define technology as any physical device or technique implemented in physical form that is specifically used to help ensure the critical information characteristics are maintained through any of the information states. Technology can be implemented in hardware, firmware, or software. It could be a biometric device, cryptographic module, or security-enhanced operating system. When we think of a thing, which could be used to protect the critical characteristics of information, we are thinking of technology.

Usually organizations are built around functional responsibilities. The advent of computer technology created the perception that a group needed to be established to accommodate the new machines that would process, store, and transmit much of our vital information. In other words, the organization was adapted to suit the evolving technology. Is this wrong? Not necessarily; however, it is possible to create the impression that technology exists for technology's sake. Telecommunications and computer systems are simply media for information. The media need to be adapted to preserve certain critical characteristics with the adaptation and use of the information media (technology). Adaptation is a design problem, but use and application concerns bring us to the next layer.

POLICY AND PRACTICE

The second layer of the third dimension is that of policy and practice. It's the recognition of the fact that information systems security is not just a product that will be available at some future date. Because of our technology focus, it's easy to begin to think of security solutions as devices or add-on packages for existing information systems. We are guilty of waiting for technology to solve that which is not solely a technological problem. Having an enforceable (and enforced) policy can aid immeasurably in protecting information.

A study has shown 75% of federal agencies don't have a policy for the protection of information on PC-based information systems [OTA87]. Why, if it is so effective, is policy such a neglected security measure? It may be due in part to the evolving social and moral ethic with regard to our use of

information systems. The proliferation of unauthorized software duplication is just another symptom of this problem. Even though software companies have policies and licensing caveats on their products, sanctions and remedies allowed by law are difficult if not impossible to enforce. No major lawsuit involving an individual violator has come before our courts, and it appears many people don't see the harm or loss involved. Although there are limits established by law, it seems we as "society" accept a less stringent standard.

Closely associated with the matter of policy is that of practice. A practice is a procedure we employ to enhance our security posture. For example, we may have a policy that states that passwords must be kept confidential and may only be used by the uniquely-authenticated user. A practice, which helps ensure this policy is followed, would be committing the password to memory rather than writing it somewhere.

The first two layers of the third dimension represent the design and application of a security-enhanced information system. The last building block of our model represents the understanding necessary to protect information. Although an integral aspect of the preceding two layers, it must be considered individually as it is capable of standing alone as a significant security measure.

EDUCATION, TRAINING, AND AWARENESS

The final layer of our third dimension is that of education, training, and awareness. As you will see, were the model laid on its back like a box, the whole model would rest on this layer. This phenomenon is intentional. Education, training, and awareness may be our most prominent security measures, for only by understanding the threats and vulnerabilities associated with our proliferating use of automated information systems can we begin to attempt to deal effectively with other control measures.

Technology and policy must rely heavily on education, training, and awareness from numerous perspectives. Our upcoming engineers and scientists must understand the principles of information security if we expect them to consider the protection of information in the systems they design. Currently, nearly all university graduates in computer science have no formal introduction to information security as part of their education [HIG89].

Those who are responsible for promulgating policy and regulatory guidance must place bounds on the dissemination of information. They must ensure information resources are distributed selectively and securely. The issue is ultimately one of awareness. Ultimate responsibility for its protection rests with those individuals and groups that create and use this information; those who use it to make critical decisions must rely on its confidentiality, integrity, and availability. Education, training and awareness promises to be the most effective security measure in the near term.

Which information requires protection is often debated in government circles. One historic problem is the clash of society's right to know and an individual's right to privacy. It's important to realize that these are not bipolar concepts. There is a long continuum that runs between the beliefs that information is a free flowing exchange of knowledge and that it is intelligence that must be kept secret. From a governmental or business perspective, it must be assumed that all information is intelligence. The question is not should information be protected, but how do we intend to protect the confiden-tiality, integrity, and availability of it within legal and moral constraints?

THE MODEL

OVERVIEW

The completed model is depicted below. There are nine distinct boxes, each three layers deep. All aspects of information systems security can be viewed within the framework of the model. For example, we may cite a cryptographic module as technology that protects information in its transmission state. What many information system developers fail to appreciate is that for every technology control there is a policy (sometimes referred to as doctrine) that dictates the constraints on the application of that technology. It may also specify parameters that delimit the control's use and may even cite degrees of effectiveness for different applications. Doctrine (policy) is an integral yet distinct aspect of the technology. The third layer--education, training, and awareness then functions as a catalyst for proper application and use of the technology based on the policy (practice) application.

Not every security measure begins with a specific tech- nology. A simple policy or practice often goes a long way in the protection of information assets. This policy or practice is then effected by communicating it to employees through the education, training and awareness level alone. This last layer is ultimately involved in all aspects of the information systems security model. The model helps us understand the comprehensive nature of information security.

CHART GOES HERE
Call Secretariat for copy of drawing

ANNEX TO
NSTISSI No. 4011

USE OF THE MODEL

The model has several significant applications. Initially, the two-dimensional matrix is used to identify information states and system vulnerabilities. Then, the three layers of security measures can be employed to minimize these vulnera-bilities based on a knowledge of the threat to the information asset. Let's take a brief look at these applications.

A developer would begin using the model by defining the various information states within the system. When an information state is identified, one then works down the vertical path to address all three critical information characteristics identifying the vulnerabilities. Once vulnerabilities are noted in this fashion, it becomes a simple matter of working down through the three layers of security measures. If a specific technology is available, the designer knows that policy and practice, as well as education, training, and awareness will be logical follow-on aspects of that control. If a technology cannot be identified, then policy/practice must be viewed as the next likely avenue. If none of the first two layers can satisfactorily counter the vulnerability then, as a minimum, an awareness of the weakness becomes important and fulfills the dictates of the model at the third layer.

Another important application is realized when the model is used as an evaluation tool. As in the design and development application, the evaluator first identifies the different information states within the system. These states can be identified separately from a specific technology. A valuable aspect of the model is the designer need not consider the medium.

After identifying all the states, an evaluator or auditor can perform a comprehensive review much the same way the systems designer used the model during the development phase. For each vulnerability discovered, the same model is used to determine appropriate security measures. It is important to note that a vulnerability may be left unsecured (at an awareness level in the third layer) if the designer or evaluator determines no threat to that vulnerability exists. Although no security practitioner should be satisfied with glaring vulnerabilities, a careful study of potential threats to the information may disclose that the cost of the security measure is more than the loss should the vulnerability be exploited. This is one of the subtle compromises alluded to earlier.

The model can also be used to develop comprehensive information systems security policy and guidance necessary for any organization. With an accurate understanding of the relation of policy to technology and education, training, and awareness, you can ensure your regulations address the entire spectrum of information security. It's of particular importance that corporate and government regulations not be bound by technology. Use of this model allows management to structure its policy outside the technology arena.

The model functions well in determining requirements for education, training, and awareness. Since this is the last layer, it plays a vital role in the application of all the security measures. Even if a designer, evaluator, or user determines to ignore a vulnerability (perhaps because of a lack of threat), then the simple acknowledgement of this vulnera-bility resides in the last layer as "awareness." Ultimately, all technology, policies, and practices must be translated to the appropriate audience through education, training, and awareness. This translation is the vehicle that makes all security measures effective. For a more complete understanding of the nuances of education, training, and awareness see [MAC89].

The 27 individual "cubes" created by the model can be extracted and examined individually. This key aspect can be useful in categorizing and analyzing countermeasures. It's also a tool for defining organizational responsibility for information security. By considering all 27 such "cubes", the analyst is assured of a complete perspective of all available security measures. This model connotes a true "systems" viewpoint.

CONCLUSION

The information systems security model acknowledges information, not technology, as the basis for our security efforts. The actual medium is transparent in the model. This eliminates unnecessary distinctions between Communications Security (COMSEC), Computer Security (COMPUSEC), Technical Security (TECHSEC), and other technology-defined security sciences. As a result, we can model the security relevant processes of information throughout an entire information system--automated or not.

This model responds to the need for a theoretical foundation for modeling the information systems security sciences. The process begins now by acknowledging the central element in all our efforts--information. Only when we build on this foundation will we accurately address the needs of information systems security in the next decade and beyond.

REFERENCES

[CHR90] Interview with Agent Jim Christy, Chief, Air Force Office of Special Investigations, Computer Crime Division, 26 March 1990.

[DOD85] Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, Department of Defense, Washington, DC, December 1985.

[DOJ88] Basic Considerations in Investigating and Proving Computer-Related Federal Crimes, U.S. Department of Justice, Justice Management Division, Washington, DC, November 1988.

[HIG89] Higgins, John C., Information Security as a Topic in Undergraduate Education of Computer Scientists, Proceedings of the 12th National Computer Security Conference, November 1989.

[MAC89] Maconachy, W.V., Computer Security Education, Training, and Awareness: Turning a Philosophical Orientation into Practical Reality, Proceedings of the 12th National Computer Security Conference, November 1989.

[OTA87] U.S. Congress, Office of Technology Assessment, Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information, OTA-CIT-310, Washington, DC, U.S. Government Printing Office, October 1987.

[PFL89] Pfleeger, Charles P., Security in Computing, Prentice-Hall, 1989.